ENCIPHERED DATA DECODING DEVICE

Patent Number: JP11039156
Publication date: 1999-02-12
Inventor(s): SASAKI SHIGEHIKO
Applicant(s): FUJI XEROX CO LTD
Requested Patent: ☐ JP11039156
Application Number: JP19970195451 19970722
Priority Number(s):
IPC Classification: G06F9/06; G06F12/14; G06F12/14; G09C1/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To prevent encipherment-protected data from being illegally used due to an altered decoding support program.
SOLUTION: Receiving a decoding instruction, a decoding device 100 temporarily stops operation of a CPU. An address detection part 103 monitors memory accessing of the CPU and acquires a store address Pr of an instruction code that issues the decoding instruction. A cipher authentication part 102 authenticates a cipher key. A decoding support program authentication part 104 acquires the authentication range designation (pre, post) from the cipher key, calculates a message summary number using a unidirectional hash function about an area covering Pr-pre through Pr+post, and compares the calculation result with the message summary number contained in the cipher key to authenticate the correctness of the decoding support program. When this authentication succeeds, a data decoding part 101 acquires a cipher decoding key from the cipher key and decodes the enciphered data.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－39156

(43)公開日　平成11年(1999)２月12日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ａ
					５５０Ｚ
	12/14	３１０		12/14	３１０Ｚ
		３２０			３２０Ｂ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ

審査請求　未請求　請求項の数11　ＯＬ　（全９頁）

(21)出願番号　特願平9－195451

(22)出願日　平成９年(1997)７月22日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　佐々木　茂彦
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

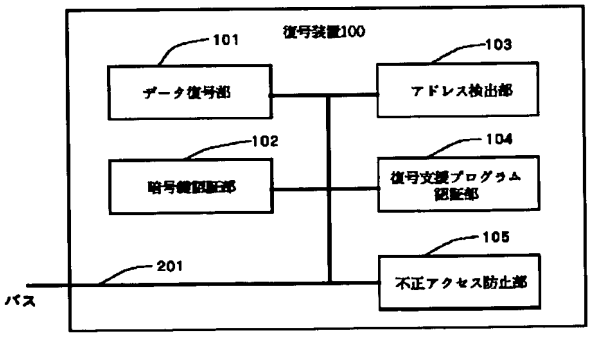
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　暗号化データ復号装置

(57)【要約】

【課題】　復号支援プログラムの改竄により、暗号でプロテクトしたデータが不正に流用されることを防止する。

【解決手段】　復号指示を受けた復号装置１００は、ＣＰＵ２０２の動作を一時停止させる。アドレス検出部１０３は、ＣＰＵ２０２のメモリアクセスを監視し、復号指示発行の命令コードの格納アドレスＰｒを取得する。暗号認証部１０２は、暗号鍵３０３の認証を行う。復号支援プログラム認証部１０４は、暗号鍵３０３から検証範囲指定（ｐｒｅ、ｐｏｓｔ）を取得し、Ｐｒ－ｐｒｅからＰｒ＋ｐｏｓｔまでの領域について、一方向ハッシュ関数を用いたメッセージ要約数を算出し、この算出結果を、暗号鍵３０３中のメッセージ要約数５０２と比較し、復号支援プログラムの正当性を認証する。認証成功時、データ復号部１０１が、暗号鍵３０３から暗号の復号鍵５０１を取得し、暗号化データを復号する。



【特許請求の範囲】
【請求項１】コンピュータ・システムに実装されて暗号化されたデータを復号する暗号化データ復号装置おいて、
暗号化されたデータを暗号鍵に基づき復号するデータ復号手段と、
上記暗号鍵が正当なものであることを認証する暗号鍵認証手段と、
ＣＰＵから復号指示の受取ったとき、復号支援プログラム中の上記復号指示を出した命令コードのメモリ・アドレスを検出するアドレス検出手段と、
上記命令コードのメモリ・アドレスに基づいて上記復号支援プログラムが正当なものであることを認証する復号支援プログラム認証手段とを有することを特徴とする暗号化データ復号装置。
【請求項２】上記復号支援プログラムの実行中に割込み等で不正に処理の流れを奪われた場合に、それを検知し対抗処置をとる不正アクセス防止手段をさらに有する請求項1 記載の暗号化データ復号装置。
【請求項３】上記復号支援プログラム認証手段は、上記命令コードのメモリ・アドレスにより決定される所定のメモリ・アドレス範囲のコードの内容が真正なものであるかどうかを検証する請求項1 または2 記載の暗号化データ復号装置。
【請求項４】上記所定のメモリ・アドレス範囲のコードの内容の所定の関数による計算結果に基づいて上記所定のメモリ・アドレス範囲のコードの内容が真正なものであることを検証する請求項3 記載の暗号化データ復号装置。
【請求項５】上記所定の関数を所定の一方向性関数とする請求項4 記載の暗号化データ復号装置。
【請求項６】上記暗号鍵は、真正な復号支援プログラムから生成した参照値を保持し、上記復号支援プログラム検証手段による計算結果と、上記暗号鍵が保持する上記計算結果とを比較して上記復号支援プログラムの正当性が認証される請求項4 または5 記載の暗号化データ復号装置。
【請求項７】上記暗号鍵は、上記所定のメモリ・アドレス範囲を指定する情報をさらに保持し、上記参照値は指定されたメモリ・アドレス範囲に基づいて生成される請求項6 記載の暗号化データ復号装置。
【請求項８】コンピュータ・システムに実装されて暗号化されたデータを復号する暗号化データ復号装置おいて、
暗号化されたデータを暗号鍵に基づき復号するデータ復号手段と、
ＣＰＵから所定の情報がバスに転送されたとき、復号支援プログラム中にある、上記所定の情報を上記バスに転送した命令コードのメモリ・アドレスを検出するアドレス検出手段と、
上記命令コードのメモリ・アドレスにより決定される所定のメモリ・アドレス範囲の上記復号支援プログラムの内容に基づいて上記復号支援プログラムが正当なものであることを認証する復号支援プログラム認証手段とを有することを特徴とする暗号化データ復号装置。
【請求項９】暗号化データを復号する暗号鍵本体と、上記暗号化データを復号するために用いる復号支援プログラムの所定の範囲のコードの所定の関数による計算結果と、上記暗号化鍵本体および上記計算結果に対する署名とを含む暗号鍵情報を生成する暗号鍵情報生成装置。
【請求項１０】暗号化データを復号する暗号鍵本体と、上記暗号化データを復号するために用いる復号支援プログラムの所定の範囲のコードの所定の関数による計算結果と、上記暗号化鍵本体および上記計算結果に対する署名とを含む暗号鍵情報を受け取るステップと、
暗号化データを復号するときに、復号に用いる復号支援プログラムの上記所定の範囲に対応するメモリ領域に展開されたコードを取り出すステップと、
上記取り出されたコードの上記所定の関数による計算結果を生成するステップと、
生成された上記計算結果と、上記暗号鍵情報中の上記計算結果とを比較するステップと、
上記比較の結果に基づいて、上記復号に用いる復号支援プログラムの真正を検証するステップとを有することを特徴とする復号支援プログラム検証方法。
【請求項１１】バスと、
上記バスに接続されたＣＰＵと、
上記バスに接続されたメモリと、
上記バスに接続された認証装置とを有し、
上記認証装置は、
上記ＣＰＵから暗号化データの復号指示が上記バスを介して転送されたとき、復号支援プログラム中にある、上記復号指示を出した命令コードのメモリ・アドレスを検出するアドレス検出手段と、
上記命令コードのメモリ・アドレスに基づいて上記復号支援プログラムが正当なものであることを認証する認証手段とを有することを特徴とするコンピュータ・システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、暗号化されたデータを復号する技術に関するものである。
【０００２】
【従来の技術】従来、暗号方式をコンピュータ・システムに適用し、暗号化されたプログラムやデータを復号して利用する場合には、そのシステムの上で動作する復号プログラム（復号計算およびそれを支援するプログラム）を実行するのが一般的である（特開平3 －６８０２４号公報）。ところで、仕様が公開されたオープンなコンピュータ・システムにおいては、プログラムの解析お

よび改変が容易であるため、復号プログラムの復号支援部分（以下、復号支援プログラムともいう）を改変することにより、元の復号プログラムの仕様に反して、復号したデータを不正に利用することが簡単にできてしまい、システム全体の安全性は低くなるという問題があった。暗合方式の進歩はめざましく、強力な暗号強度をもつ暗号方式が多く提案されている。しかし、復号プログラムの解析、改変による問題は、使用している暗号方式の安全性には依存しないため、いくら高い強度をもつ暗号方式を採用しても、解決することはできない。

【０００３】この問題を解決しようとする提案として、復号プログラム自体を暗号化し、データ復号時にのみ復号プログラムを復号して、データ復号作業を行う手段を採用し、これにより、復号プログラムの解析および改変を困難にするものが知られている（特開平9－６２３２号公報）。しかし、復号プログラムを復号するのも、結局プログラムによって行われるため、本質的な解決になっておらず、解析と改変に要するコストを多少増加させるという効果しかない。しかも、近年のコンピュータの性能向上を考慮すると、増加するコストは大きな障害とはなり得ないため、復号プログラムの解析と改変を効果的に防止することができないという問題がある。また、いったん復号プログラムの改変に成功してしまえば、改竄プログラムの実行を防ぐことはできず、意図しない目的への復号したデータの流用の防止ができないという問題がある。

【０００４】また、復号プログラムの改変を防止する手段として、ＣＰＵがメモリにアクセスするアドレスを監視して、予想される正当な復号プログラムのメモリアクセスパターンと比較した結果、正当と判断した場合は、メモリアクセスを許可するが、不正と判断した場合には、メモリアクセスを遮断することにより、意図しない不正なデータ利用を防止する提案がある（特開平5－３２４４８３号公報）。しかし、機器組込用のプログラムがＲＯＭで供給されるような特殊な小規模システムならば、プログラムは固定したアドレス位置に存在するため、ＣＰＵがアクセスするアドレスを監視することにより、復号プログラムの正当性の判断が可能だが、一般的なシステムでは、プログラムのロードされるアドレスは動的に決定されるため、アクセスするアドレス情報で復号プログラムを判定することができないという問題がある。また、不正判定基準のアクセスパターンを容易に変更することができないので、拡張性に乏しく、多くの暗号化データに対応することが難しい。そのため、この手法は一般的なコンピュータ・システムにおいて、使用することはできないという問題がある。

【０００５】以上に述べたとおり従来の技術では、一般的なコンピュータ・システムにおいて、復号プログラムが改変されていない正当なものであることを、復号時に認証することができず、この結果、改変された復号プログラムの実行を防ぐことができないかった。このため、改竄、改変された復号プログラムによる、復号したデータの意図しない目的への流用を効果的に防止できない。そのため、暗号方式の強度にかかわらず、システム全体の安全性は低くなってしまうという問題がある。

【０００６】

【発明が解決しようとする課題】本発明は、仕様が公開されたオープンなコンピュータ・システムにおいても、復号プログラムの正当性を暗号化データの復号時に認証できるようにし、これにより、改竄された復号プログラムによる意図しない目的への復号したデータの流用を防止することを課題としている。

【０００７】

【課題を解決するための手段】本発明によれば、上述の目的を達成するために、コンピュータ・システムに実装されて暗号化されたデータを復号する暗号化データ復号装置に、暗号化されたデータを暗号鍵に基づき復号するデータ復号手段と、上記暗号鍵が正当なものであることを認証する暗号鍵認証手段と、ＣＰＵから復号指示の受取ったとき、復号支援プログラム中にある、上記復号指示を出した命令コードのメモリ・アドレスを検出するアドレス検出手段と、上記命令コードのメモリ・アドレスに基づいて上記復号支援プログラムが正当なものであることを認証する復号支援プログラム認証手段とを設けるようにしている。

【０００８】この構成においては、復号支援プログラム中の復号指示を出した命令コードのメモリ・アドレスに基づいて、例えば、予め定められた領域のコードの内容を検証し、復号支援プログラムの正当性を認証できる。この場合、復号支援プログラムがメモリのどの領域にロードされていても検出した命令コードのアドレスを利用して適合化できる。

【０００９】

【発明の実施の態様】つぎに、本発明の実施例について、図面を参照して説明する。図1は、本発明の復号装置を用いて暗号化データを復号するコンピュータ・システムを示している。この実施例においては、コンピュータ・システムに実装された復号装置１００と、コンピュータ・システムで実行される復号支援プログラムとにより暗号化データの復号を行う。

【００１０】図1において、内部バス２０１に、ＣＰＵ２０２、Ｉ／Ｏ部２０３、復号装置１００、およびメモリ２０５を接続して、コンピュータ・システムが構成される。ＣＰＵ２０２は、一般的なストアードプログラム方式のもので、メモリ２０５に格納されたプログラムコードを、内部バス２０１を介して読取って解釈を行い、読取ったプログラムコードの指示に従い動作する。システムの利用者は、ＣＰＵ２０２に内部バス２０１を介して、Ｉ／Ｏ部２０３とメモリ２０５に格納されたデータに、アクセスするよう、プログラムで指示を与えること

により、意図する通りにシステムを利用することができる。

【００１１】図2は、図1の復号装置１００の構成例を示す。この図において、復号装置１００は、データ復号部１０１、暗号鍵認証部１０２、アドレス検出部１０３、復号支援プログラム認証部１０４、および不正アクセス防止部１０５を含んで構成されている。データ復号部１０１は、暗号化されたデータを暗号鍵に基づき復号するものである。暗号鍵認証部１０２は、その暗号鍵３０３（図5）が正当なものであることを認証するものである。アドレス検出部１０３は、ＣＰＵ２０２から復号の指示の受取ったとき、復号支援プログラム３０１（図3）中にある、その復号指示を出した命令コードのメモリ・アドレスを検出するものである。復号支援プログラム認証部１０４は、復号支援プログラム３０１が正当なものであることを認証するものである。また、不正アクセス防止部１０５は、復号支援プログラム３０１の実行中に割込み等で不正に処理の流れを奪われた場合に、それを検知し対抗処置をとるものである。

【００１２】図3は、暗号化されたデータを復号するときの、メモリ内のデータ格納状況を表したものである。図3において、復号支援プログラム３０１は、暗号化されたデータ３０２を復号して、復号データ格納領域３０４に格納するよう復号装置１００に指令を出し、意図した目的のために復号データを利用するプログラムである。暗号鍵３０３（図5参照）は、暗号化データを復号するために必要な鍵データである。復号支援プログラム３０１、暗号化されたデータ３０２、暗号鍵３０３、復号データ格納領域３０４のメモリ２０５における格納アドレスは、ｐ、ｃ、ｋおよびｄである。

【００１３】図4は、復号支援プログラムのメモリ格納状態の概念図である。図4において、メモリ２０５上の、アドレスｐからp_{end}までが復号支援プログラム３０１が格納される領域である。復号支援プログラム３０１の中には、復号装置２０４に復号指示を発行する、復号指示発行部分４０２が含まれ、このコードが格納されるアドレスはｐｒである。復号指示発行部分４０２のアドレスｐｒから、前にｐｒｅバイト、後ろにｐｏｓｔバイトで区切ったブロックが、復号支援プログラム検証ブロック４０３である。復号支援プログラム検証ブロック４０３のメッセージ要約数を用いて、復号支援プログラムの正当性を判断する。ｐｒｅとｐｏｓｔは、暗号鍵３０３で指定される（図5参照）。

【００１４】図5は、暗号鍵３０３の構成図である。暗号鍵３０３はデジタルデータであり、暗号の復号鍵５０１、復号支援プログラムのメッセージ要約数５０２、検証領域範囲指定５０３、および暗号鍵全体の署名５０４から構成される。

【００１５】図6は、暗号鍵３０３を生成する暗号鍵生成装置の構成例を示しており、図6において、暗号鍵生成装置は検証範囲指定部５０５、復号支援プログラム入力部５０６、復号鍵入力部５０７、メッセージ要約数生成部５０８、署名生成部５０９および暗号鍵出力部５１０を含んで構成されている。検証範囲指定部５０５は、復号指示コードのアドレス、検証ブロックを特定するバイト数ｐｒｅおよびｐｏｓｔを受け取る。メッセージ要約数生成部５０８は、検証範囲指定部５０５で指定された範囲で復号支援プログラムのメッセージ要約数を生成する。署名生成部５０９は、復号鍵入力部５０７から入力された復号鍵、検証ブロック指定情報のバイト数ｐｒｅおよびｐｏｓｔおよびメッセージ要約数生成部５０８で生成したメッセージ要約数に対して署名を生成する。暗号鍵出力部５１０は、復号鍵、メッセージ要約数、ブロック指定情報のｐｒｅおよびｐｏｓｔ、署名を一体にして出力する。

【００１６】つぎに、本実施例の復号処理について説明する。本実施例では、復号処理は復号支援プログラム３０１および復号装置１００が共同して行う。図7は、復号支援プログラム３０１のフローチャートである。図8は、復号装置１００の処理の流れを表すフローチャートである。図7において、暗号化データを復号するために、復号支援プログラム３０１の実行が開始されると、まず前処理が行われる（ステップ６０１）。前処理では、暗号化データ３０２と暗号鍵３０３をメモリ２０５にロードし、復号データを格納する領域３０４を確保して、図3に示す通りにメモリ格納状況を構成する作業や、その他の必要な前処理作業を行う。次に、暗号鍵の格納アドレスｋ、暗号化データの格納アドレスｃ、復号データの指定格納アドレスｄを復号装置１００に与える。具体的には内部バス２０１を通じて、復号装置１００にマップされたＩ／Ｏアドレスに、ｋ、ｃ、ｄを出力することにより行う（ステップ６０２）。もちろん、別の方法で復号装置１００と通信しても構わない。

【００１７】この後、復号装置１００に復号処理を行うよう指示を発行する（ステップ６０３）。このとき、ステップ６０３に相当する命令コードが格納されているアドレスがＰｒである。この指示の発行は、具体的には、内部バス２０１を通じて、復号装置１００にマップされたＩ／Ｏアドレスに、指示命令を出力することにより行われる。

【００１８】復号を行う復号装置１００は、内部バス２０１を介して、ＣＰＵ２０２がどのようなアクセスをしているかを、監視することができる。また、ＣＰＵを介さずに直接メモリにアクセス（ＤＭＡ：Ｄｉｒｅｃｔ Ｍｅｍｏｒｙ Ａｃｃｅｓｓ）することができる。加えて、ＣＰＵ２０２の動作を制御し、必要に応じてＣＰＵ２０２を一時停止状態に保ったり、動作を再開させることができる。

【００１９】図8において、復号指示を受けた復号装置１００は、ステップ７０１において、ただちにＣＰＵ２

０２の動作を一時停止させ、暗号鍵３０３の格納アドレスｋ、暗号化データ３０２の格納アドレスｃ、復号データの指定格納アドレスｄを読取る（ステップ７０１）。これにより復号支援プログラム３０１はステップ６０３で一時停止状態となる。以下の復号装置１００のメモリ２０５へのアクセスはすべてＤＭＡを用いる。

【００２０】復号装置１００の処理はステップ７０２に進む。ステップ７０２では、ＣＰＵ２０２のメモリ２０５へのアクセスの監視によって、復号指示発行の命令コードの格納アドレスＰｒを取得する。

【００２１】次にステップ７０３において、暗号鍵３０３の認証を行う。暗号鍵３０３には、暗号鍵全体の署名５０４が用意されており、電子書名認証技術により、正当な暗号鍵であるか認証する。具体的には、復号装置には署名認証鍵が用意されており、ＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｅｌｍａｎ）公開鍵暗号技術と、一方向ハッシュ関数を用いたメッセージ要約生成技術を用いて認証を行う。もちろん、他の方式で認証しても構わない。

【００２２】もし認証に失敗した場合は、暗号鍵３０３が改竄されている可能性がある。復号装置１００は、暗号鍵３０３が正当なものでないと見なし、ステップ７０５に進む。ステップ７０５において、ＣＰＵ動作を再開させ、ＣＰＵに「暗号鍵の認証に失敗」を意味するエラーコードを返す。具体的には、復号装置１００にマップされたＩ／Ｏアドレスにアクセスすることにより、ＣＰＵ２０２が読出すことができるレジスタにエラーコードを格納する。もちろん、別の方法でＣＰＵ２０２と通信しても構わない。動作を再開した復号支援プログラム３０１では、ステップ６０５の分岐でエラーが発生したと判断し、ステップ６０６でエラー処理を行い、復号を行わずに終了する。

【００２３】ステップ７０３において暗号鍵３０３の認証に成功した場合は、ステップ７０４へ処理を進める。ステップ７０４において、暗号鍵３０３から検証範囲指定５０３を取得し、Ｐｒ－ｐｒｅからｐｒ＋ｐｏｓｔまでの領域について、一方向ハッシュ関数を用いたメッセージ要約数を算出する。

【００２４】続いて、ステップ７０６において、暗号鍵３０３中の復号支援プログラムの検証領域のメッセージ要約数５０２と、前ステップ７０４で算出したメッセージ要約数を比較する。もしこれらが一致しなかった場合、ＣＰＵ２０２が実行している復号支援プログラム３０１が、暗号鍵３０３の発行者が意図したものと異なることを意味する。復号装置１００は、復号支援プログラム３０１が改竄されたものと見なして、ステップ７０７に進む。ステップ７０７において、ＣＰＵ２０２の動作を再開させ、ＣＰＵに「復号支援プログラムの認証に失敗」を意味するエラーコードを返す。具体的には、復号装置１００にマップされたＩ／Ｏアドレスにアクセスすることにより、ＣＰＵ２０２が読出すことができるレジスタにエラーコードを格納する。もちろん、別の方法でＣＰＵ２０２と通信しても構わない。動作を再開した復号支援プログラム３０１は、図7のステップ６０５の分岐でエラーが発生したと判断し、ステップ６０６でエラー処理を行い、復号を行わずに終了する。

【００２５】図8のステップ７０６で復号支援プログラムの認証に成功した場合は、ステップ７０８へ処理を進める。ステップ７０８において、復号装置１００は、暗号鍵３０３から暗号の復号鍵５０１を取得して、暗号化されたデータの復号処理を行う。具体的には、暗号の復号鍵と復号装置の装置ごとに別々のものが用意されている秘密鍵の2つから、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）等のブロック暗号の復号鍵を生成し、ブロック暗号復号器に、ＤＭＡで暗号化されたデータを読出し、復号結果をＤＭＡで復号データ領域に書出す。もちろん、どのような方法の暗号／復号方式を用いても構わない。

【００２６】復号処理が終わった後は、ステップ７０９に進み、復号したデータを利用する。利用後は必要に応じて、復号したデータをメモリ２０５から消去することにより、意図しない目的に復号したデータを用いられることを防止できる。

【００２７】また、復号装置１００は、ＣＰＵ２０２の内部バス２０１へのアクセスを監視することにより、復号支援プログラム３０１がＣＰＵ２０２により実行されている間に不正な割込み等により処理の流れを奪う操作を検知できる。不正に処理の流れが奪われたことを検知した場合、復号作業を即刻中止し、それまでに復号したデータもＤＭＡにより破壊する。この機能により、ハードウェア割り込みによるプログラムの動作への干渉を排除することができ、さらに安全性が向上する。

【００２８】

【発明の効果】以上説明したように本発明は、復号支援プログラムの正当性を、復号時にチェックすることにより、改竄された復号支援プログラムによる意図しない目的への復号したデータの流用を防止する。これにより、復号支援プログラムの耐改変性を高めることができ、暗号強度に見合ったシステムの安全性を得ることができる。

【図面の簡単な説明】

【図１】本発明の実施例のコンピュータ・システムの構成を示すブロック図である。

【図２】上述実施例の復号装置の構成を示すブロック図である。

【図３】暗号化されたデータを復号するときのメモリ内のデータ格納状況を説明する図である。

【図４】復号支援プログラムのメモリ格納状態の概念的に示す図である。

【図５】暗号鍵の構成を説明する図である。

【図6】 暗号鍵を生成する暗号鍵生成装置の構成例を示すブロック図である。

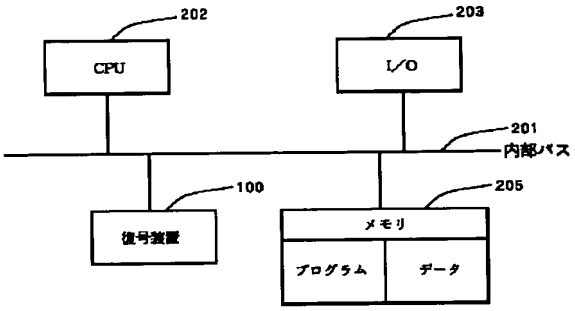
【図7】 復号支援プログラムの動作を説明するフローチャートである。

【図8】 復号装置の処理の流れを説明するフローチャートである。

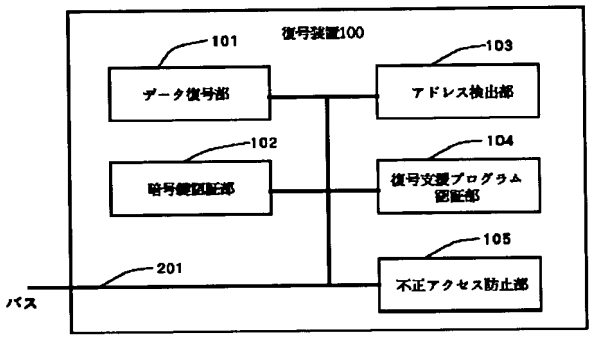
【符号の説明】

１００ 復号装置
１０１ データ復号部
１０２ アドレス検出部
１０３ 復号支援プログラム認証部
１０４ 不正アクセス防止部
２０１ バス
２０２ ＣＰＵ
２０３ Ｉ／Ｏ部
２０５ メモリ

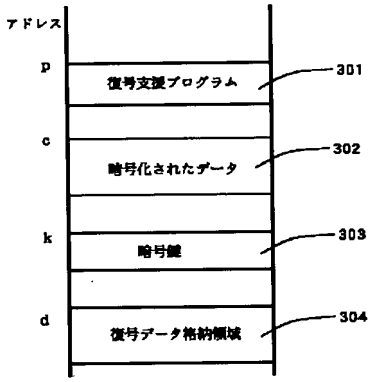
【図1】



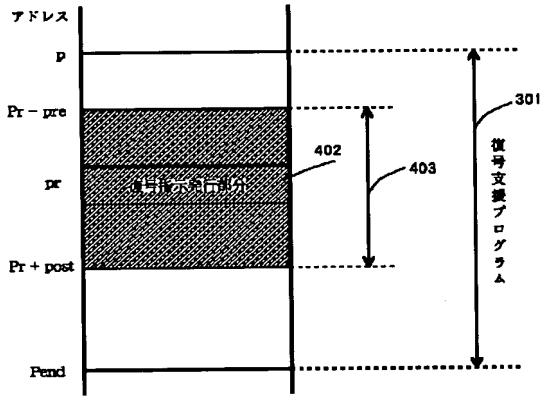
【図2】



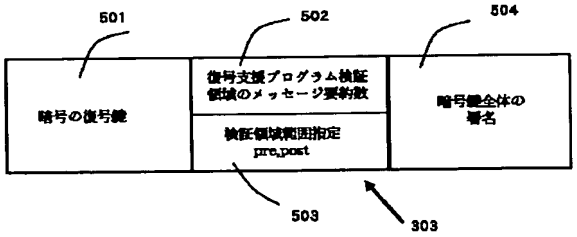
【図3】



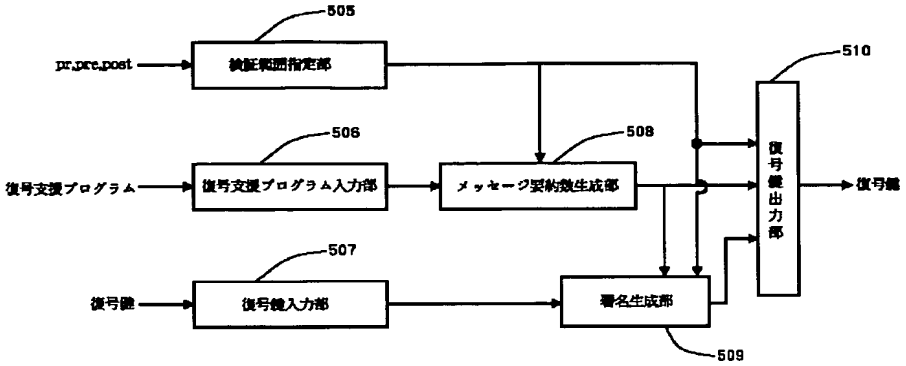
【図4】



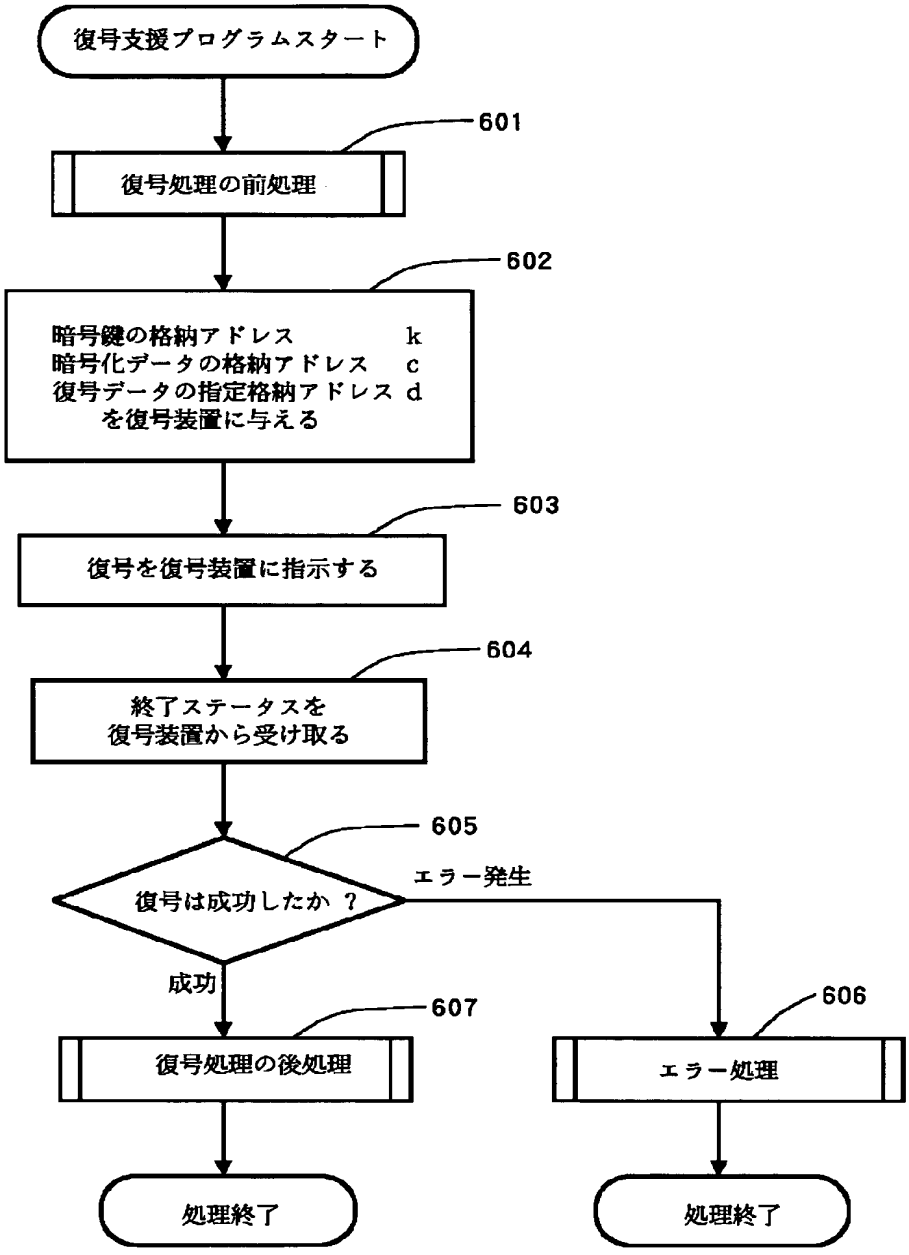
【図5】



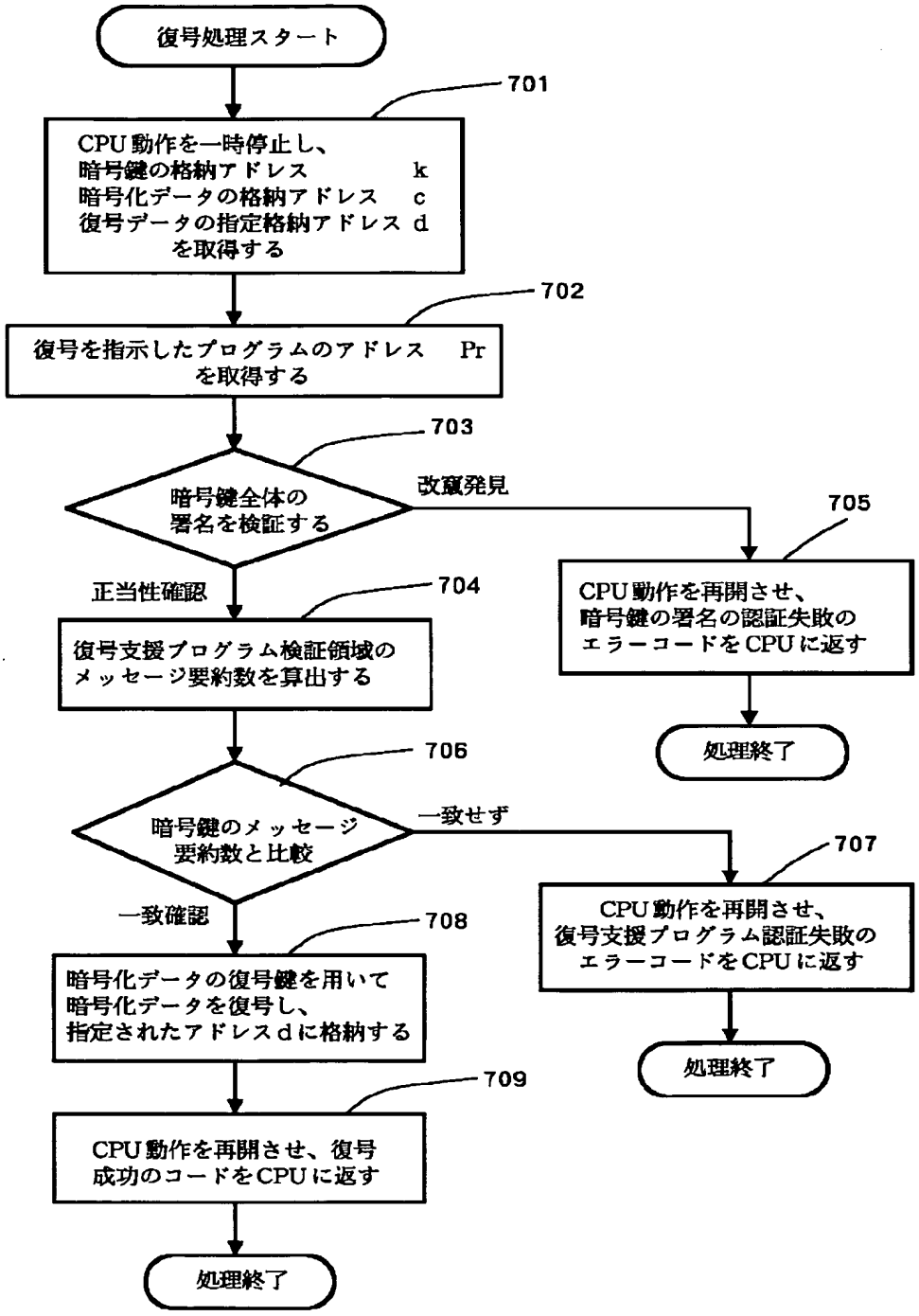
【図6】


505
pr,pre,post
検証範囲指定部
506
復号支援プログラム
復号支援プログラム入力部
508
メッセージ要約値生成部
510
復号鍵出力部
復号鍵
507
復号鍵
復号鍵入力部
署名生成部
509

【図7】


復号支援プログラムスタート
601
復号処理の前処理
602
暗号鍵の格納アドレス　k
暗号化データの格納アドレス　c
復号データの指定格納アドレス　d
を復号装置に与える
603
復号を復号装置に指示する
604
終了ステータスを
復号装置から受け取る
605
復号は成功したか ？
エラー発生
成功
607
復号処理の後処理
606
エラー処理
処理終了
処理終了

【図8】


復号処理スタート
701
CPU動作を一時停止し、
暗号鍵の格納アドレス k
暗号化データの格納アドレス c
復号データの指定格納アドレス d
を取得する
702
復号を指示したプログラムのアドレス Pr
を取得する
703
暗号鍵全体の
署名を検証する
改竄発見
705
CPU動作を再開させ、
暗号鍵の署名の認証失敗の
エラーコードをCPUに返す
処理終了
正当性確認
704
復号支援プログラム検証領域の
メッセージ要約数を算出する
706
暗号鍵のメッセージ
要約数と比較
一致せず
707
CPU動作を再開させ、
復号支援プログラム認証失敗の
エラーコードをCPUに返す
処理終了
一致確認
708
暗号化データの復号鍵を用いて
暗号化データを復号し、
指定されたアドレスdに格納する
709
CPU動作を再開させ、復号
成功のコードをCPUに返す
処理終了